PROCURADURÍA AGRARIA

Secretaría General

Dirección de Informática

Manual de Seguridad Informática
Centro de Cómputo

(Políticas y lineamientos)

CONTENIDO

INTRODUCCIÓN.

La Seguridad Informática está orientada a brindar protección contra las contingencias y riesgos relacionados con la infraestructura informática actualmente instalada en el Centro de Cómputo Institucional; la Seguridad Informática radica en asegurar que los elementos, servicios y recursos de los sistemas de información desarrollados para beneficio de la Institución sean empleados de forma correcta, a efecto de disponer de integridad en la información y el resguardo necesarios para proteger su estructura.

La implementación de nuevas tecnologías y la adquisición e instalación de equipamiento informático requiere de un marco normativo que aporte las medidas inherentes a la seguridad; en el cual se plasmen mecanismos que resguarden su estado físico, su accesibilidad, uso y aprovechamiento; razón por la cual, el objetivo de la Dirección de Informática es estructurar un Manual de Seguridad Informática, con la finalidad de establecer un medio documental de consulta así como normativo para implementar las acciones que aporten medidas de seguridad y conservar en óptimo estado los bienes y servicios actualmente disponibles.

En base a lo anterior, el Manual de Seguridad Informática pretender ser una herramienta de carácter administrativo y normativo, que permite concientizar a los funcionarios y usuarios sobre la adecuada y precisa observancia de cada una de las políticas y lineamientos para proteger y conservar la vida útil de la infraestructura informática institucional.

La normatividad sobre la seguridad informática incluye las medidas de protección para la generación, otorgamientos, uso, resguardo, cancelación y eliminación de claves de acceso a los diversos servicios de telecomunicaciones (red y telefonía), a los sistemas de información institucionales y a los equipos de cómputo destinados para las tareas cotidianas y la administración de servicios.

Así mismo, se establecen las sanciones a las cuales se harán acreedores los usuarios que incurran en faltas y/u omisiones a las políticas y lineamientos establecidos para otorgar las medidas de seguridad informática.

Las medidas de seguridad serán difundidas entre el personal informático, Analistas Programadores de la Estructura Territorial y los Enlaces Informáticos de Oficinas Centrales, con la finalidad de reforzar su promoción entre los usuarios, y establecer los niveles de responsabilidades y obligaciones para el adecuado empleo de los bienes y servicios informáticos.

Resulta importante resaltar la necesidad de contar con un instrumento que sirva de guía para la recuperación oportuna de la operación del Centro de Cómputo de la Institución en caso de que se presente algún contratiempo como incendio, temblor, derrumbe o cualquier otro que dañe la operación de los servicios, equipos o sistemas instalados.

OBJETIVOS.

La Procuraduría Agraria ha invertido en la adquisición e instalación de infraestructura informática destinada a brindar a los usuarios los servicios de telecomunicaciones mecanismos para apoyar sus funciones y actividades cotidianas, tales como la consulta del servicio de Internet, el acceso al servicio del Correo Electrónico, los Servidores de Red (dominio), los servicios de Telefonía, el Servidor de Respaldo de Información y el acceso a Sistemas de Información Institucional.

Los equipos de cómputo y servicios de uso específico que han sido designados con una misión crítica requieren de un área segura para su correcta instalación y óptimo funcionamiento, razón por la cual, la Dirección de Informática ha establecido el presente Manual de Seguridad Informática, con la finalidad de cubrir y cumplir los siguientes objetivos:

a. Asegurar la integridad y continuidad de los Servicios, Equipos y Sistemas de Información Institucional instalados en el Centro de Cómputo, con el apoyo de instrumentos que regulen tanto el acceso a las instalaciones del Centro de Cómputo como el ingreso a Servicios, Equipos de Cómputo y Sistemas de Información Institucional.

b. Salvaguardar la confidencialidad y configuración de los Equipos de Cómputo, Servicios de uso específico y de los Sistemas de Información Institucionales de la Procuraduria Agraria contra cualquier intento de acceso al Centro de Cómputo no autorizado o de mal uso de estos.

c. Disponer de un mecanismo de registro, control y seguimiento para la adecuada administración en la creación, actualización, cancelación, uso y resguardo de las Claves de Seguridad de Acceso a los Equipos de Cómputo, Servicios y de los Sistemas de Información Institucionales actualmente instalados en la Procuraduria Agraria, siendo estos los siguientes:

- **Servicios.-** Internet, Correo Electrónico, Red Institucional, Acceso a Servidores de Dominio, Carpetas Compartidas en Servidores y Telefonía.

- **Sistemas Informáticos.**- Cualquier sistema de cómputo o bases de datos desarrollados para la administración y explotación de información Institucional.

c. Asegurar la confidencialidad sobre el uso de claves de seguridad de acceso a equipos de cómputo, servicios y a los sistemas de información institucionales.

d. Proporcionar a las unidades administrativas de la Procuraduría Agraria los servicios de asesoría, a efecto de mantener un eficaz y eficiente manejo de las Claves de Seguridad de Acceso a los equipos de cómputo, servicios y a los sistemas de información institucionales.

e. Proporcionar a las unidades administrativas de la Procuraduría Agraria las herramientas (capacitación) informáticas para el adecuado funcionamiento de la seguridad de los equipos de cómputo, servicios y a los sistemas de información institucionales.

f. Asegurar la disponibilidad de equipos de apoyo para la protección y correcta instalación de equipos de cómputo, servicios y sistemas de información institucionales, siendo estos:

- Equipo de Aire Acondicionado.
- Equipo de Detección y Extinción de Incendios.
- Centro de Distribución de Cargas.
- Planta de Emergencia.

- Unidad de Energía Ininterrumpida.
- Equipo de Videograbación de Accesos al Centro de Cómputo.

g. Asegurar la continuidad en la disponibilidad de los equipos de cómputo, servicios y sistemas de información institucional, mediante el adecuado mantenimiento preventivo y el oportuno mantenimiento correctivo de estos.

h. Contar con un instrumento que sirva de guía para la recuperación oportuna de la operación del Centro de Computo de la Institución en caso de que se presente algún contratiempo como incendios, temblores, derrumbes o cualquier otro que dañe la operación de los servicios, equipos o sistemas instalados.

ALCANCES.

La Dirección de Informática tiene la responsabilidad de establecer políticas y lineamientos que normen y regulen las acciones inherentes al adecuado funcionamiento y seguridad de los servicios de la RedPA, así como, de la infraestructura instalada en donde residen dichos servicios y el equipo de seguridad; por lo tanto, el alcance de las políticas está dispuesta de la siguiente manera:

a. La Normatividad y Lineamientos para el Manejo de Claves de Seguridad de Acceso a Servicios y Sistemas Informáticos son de observancia general y obligatoria para todas las unidades administrativas (Oficinas Centrales y Estructura Territorial) de la Procuraduría Agraria y tienen por objeto regular la actividad en cuanto al uso, seguridad, aprovechamiento, conservación y resguardo de los servicios, sistemas informáticos y bienes de esta dependencia.

b. Invariablemente la omisión y/o incumplimiento de cualquiera de las normas y lineamientos en materia de seguridad de claves de acceso a servicios y sistemas informáticos, ameritará una sanción administrativa así como el retiro del servicio o sistema informático en caso de reincidencia por el usuario o unidad administrativa correspondiente.

EQUIPO DE CÓMPUTO.

El Manual de Seguridad del Centro de Cómputo define las políticas para la instalación y mantenimiento de los bienes informáticos en el Centro de Cómputo.

De la instalación del equipo de cómputo.

1. Los bienes informáticos asignados a la Dirección de Informática invariablemente deberán ser instalados por personal de la Subdirección de Soporte Técnico, de acuerdo a las especificaciones técnicas de los mismos.

2. En el caso de equipos de reciente adquisición, éstos serán instalados preferentemente por el personal especializado que defina el proveedor externo, con la finalidad de asegurar su correcta instalación, configuración y así asegurar las garantías del equipo adquirido.

3. La Subdirección de Soporte Técnico invariablemente resguardará, en un lugar seguro y ubicado en las instalaciones de la Dirección de Informática; los manuales, discos de instalación y demás documentación, del equipo de cómputo y Servidores instalados en el Centro de Cómputo, así mismo y en caso necesario los discos serán resguardados en la Bóveda de Seguridad Bancaria.

4. El equipo de cómputo y Servidores que tengan un uso específico y una misión crítica asignada, invariablemente estarán ubicados en el Centro de Cómputo, a efecto de disponer de seguridad física, condiciones ambientales adecuadas, alimentación eléctrica y acceso solo para el personal autorizado de la Dirección de Informática.

5. El uso y aprovechamiento de los equipos de cómputo y Servidores instalados en el Centro de cómputo será destinado únicamente para apoyar las funciones propias de la Procuraduría Agraria.

6. El resguardante del equipo de cómputo y Servidores tendrá el resguardo de todo el equipo y de los programas de cómputo instalados y autorizados, siguiendo las políticas de la Dirección de Recursos Materiales y Servicios.

7. Los movimientos de reubicación, cambio y/o baja del equipo de cómputo y Servidores deberá ser notificado, mediante oficio, indicando con precisión marca, modelo y números de inventario y serie, a la Dirección de Recursos Materiales y Servicios; en caso de baja, anexar el dictamen técnico correspondiente, para apoyar la estructuración del expediente respectivo.

8. Está totalmente prohibido, en el uso y operación del equipo de cómputo y Servidores ubicados en el Centro de Cómputo, fumar y consumir todo tipo de alimentos o bebidas.

9. El equipo de cómputo y Servidores deben estar debidamente conectados a un regulador, unidad de respaldo de energía o sistema de energía ininterrumpible.

10. Invariablemente no deben colocarse objetos sobre el equipo de cómputo y Servidores y éstos deben de estar alejados de objetos magnéticos, tales como teléfonos celulares e imanes.

Del mantenimiento del equipo de cómputo.

1. El equipo de cómputo y Servidores instalados en el Centro de Cómputo estarán contemplados en el Programa de Mantenimiento Preventivo de Bienes Informáticos, siempre y cuando haya concluido el plan de garantías correspondiente.

2. Cuando se realice el mantenimiento preventivo de los equipos de cómputo que dispongan de un uso específico y una misión crítica asignada, este debe ser notificado mediante oficio a las unidades administrativas de Oficinas Centrales y la Estructura Territorial, sobre la interrupción de los servicios de Internet, Correo Electrónico, Red, Servidores, Sistemas de Información Institucional o del Servicio de Telefonía.

3. La Dirección de Informática deberá notificar el día en que se llevará a cabo las acciones de mantenimiento, señalando la hora de interrupción de los servicios de telecomunicaciones y la hora en que reanudará al 100% su operación.

4. El Administrador de la Red debe supervisar directamente las actividades de mantenimiento preventivo a los equipos de cómputo y Servidores, con la finalidad de verificar su adecuado funcionamiento.

5. En caso de que el mantenimiento preventivo sea realizado por un proveedor externo, el personal designado para tales efectos debe portar credencial de la empresa y éste debe efectuar las actividades de mantenimiento preventivo definidas previamente por la Dirección de Informática (estipuladas en el Contrato de Mantenimiento Preventivo).

6. El Administrador de la Red invariablemente deberá realizar las pruebas necesarias para verificar el óptimo funcionamiento de los equipos de cómputo y Servidores que hayan estado sujetos a acciones de mantenimiento preventivo.

7. La Dirección de Informática debe requerir, mediante oficio dirigido a la Dirección de Recursos Materiales y Servicios, el plan de garantías y el procedimiento para requerir asesoría y asistencia técnica de los equipos de cómputo y Servidores.

8. En los casos de detectar fallas y/o problemas en el desempeño del equipo de cómputo y Servidores instalados en el Centro de Cómputo, el Administrador de la Red debe reportar de manera inmediata al Centro de Atención del fabricante para su pronta atención.

9. Las fallas y/o problemas técnicos de los equipos de cómputo y Servidores deberán ser registradas en la **Bitácora de Fallas en los servicios de la Red Institucional**.

De la reubicación del equipo de cómputo.

1. La reubicación de equipo de cómputo y Servidores invariablemente debe ser autorizada por el titular de la Dirección de Informática, previo análisis presentado por el Administrador de la Red, o bien, la adquisición e instalación de equipo nuevo.

2. La reubicación de equipo de cómputo y Servidores deberá realizarse en una fecha programada que no repercuta en las tareas cotidianas de los usuarios finales.

3. En caso de ser necesario, la reubicación de equipo de cómputo y Servidores deberá notificarse mediante oficio a las unidades administrativas de Oficinas Centrales y la Estructura Territorial sobre la interrupción del servicio que se vea afectado, a efecto de que tomen las medidas necesarias para realizar sus tareas cotidianas.

4. La reubicación del equipo de cómputo y Servidores se realizará de acuerdo a las necesidades de la Institución y la implementación de nuevas tecnologías, con la finalidad de optimizar el uso y aprovechamiento de la infraestructura informática institucional.

5. El Administrador de la Red deberá notificar al titular de la Dirección de Informática la justificación de la reubicación del equipo de cómputo y Servidores, así como, de las acciones inherentes a la reubicación y los recursos necesarios para su movimiento.

6. En caso de ser necesario, la Dirección de Informática mediante oficio, deberá solicitar el apoyo técnico del fabricante del equipo de cómputo y Servidor, para realizar de manera adecuada y segura la reubicación de los mismos.

CONTROL DE ACCESOS.

Políticas definidas para disponer de un registro, control y seguimiento a las instalaciones del Centro de Cómputo, a los equipos de cómputo y los sistemas de información institucionales.

Del acceso a las zonas restringidas.

1. La Dirección de Informática definirá, de acuerdo a su naturaleza, las zonas restringidas, con la finalidad mantener un adecuado control sobre el acceso del personal que opera el Centro de Cómputo de la Procuraduría Agraria.

2. La definición de zonas restringidas tiene la finalidad de evitar acceso no autorizados al Centro de Cómputo de la Procuraduría Agraria que pueden poner en riesgo la operación de la infraestructura informática instalada o provocar pérdida de información confidencial.

3. Las zonas restringidas en la Dirección de Informática son las áreas que ocupan las Subdirecciones de Sistemas, la Subdirección de Soporte Técnico y Telecomunicaciones, el Centro de Cómputo y el Conmutador Central de la Procuraduría Agraria.

4. El acceso a las áreas de las Subdirecciones de Sistemas y Soporte Técnico y Telecomunicaciones será autorizado por el personal adscrito a dichas áreas.

5. El acceso al Centro de Cómputo y Conmutador Central de la Procuraduría Agraria está totalmente prohibido a todo personal no autorizado y su acceso requiere invariablemente autorización del Director de Informática, del Subdirector de Soporte Técnico, o bien, del Jefe de Telecomunicaciones.

Del personal autorizado.

1. Las personas autorizadas para tener acceso al Centro de Cómputo y Conmutador Central de la Procuraduría Agraria son las siguientes:

- **a.** El Director de Informática.
- **b.** El Subdirector de Soporte Técnico.
- **c.** El Subdirector de Procesamiento de Datos.
- **d.** El Jefe de Departamento de Soporte Técnico.
- **e.** El Jefe de Departamento de Desarrollo de Sistemas.
- **f.** El Supervisor de Soporte Técnico.
- **g.** El Supervisor de Desarrollo de Sistemas.
- **h.** Técnico Especializado.

2. Cualquier personal no mencionado en la política anteriormente descrita, requiere autorización del Subdirector de Soporte Técnico y en su caso del Director de Informática para tener acceso al Centro de Cómputo de la Procuraduría Agraria.

6. Las visitas que pretendan ingresar al Centro de Cómputo, deberán contar con autorización del Subdirector de Soporte Técnico o del Director de Informática, mismas que deberán registrar su ingreso en la **Bitácora de Acceso al Centro de Cómputo**.

7. Únicamente se reciben visitan con la finalidad de efectuar algún mantenimiento al equipo de computo previamente programado, visitas especiales con carácter de proveedores de algún bien o servicio, y los Titulares de la Institución como el C. Procurador Agraria, Subprocurador o Secretario General en carácter de supervisión del área, mismas que deberán registrar su ingreso en la **Bitácora de Acceso al Centro de Cómputo**.

2. Los proveedores externos de servicios y equipos de cómputo invariablemente deben contar con autorización del Director de Informática o el Subdirector de Soporte Técnico para ingresar al Centro de Cómputo de la Procuraduría Agraria.

Del acceso y registro de visitas.

1. La Dirección de Informática es responsable de elaborar y actualizar la **Bitácora de Control de Accesos al Centro de Cómputo** de la Procuraduría Agraria, así como, de las políticas que regulen el acceso del personal adscrito a la Dirección de Informática y del personal ajeno a la Dirección y la Institución.

2. La **Bitácora de Control de Accesos al Centro de Cómputo** de la Procuraduría Agraria debe estar en lugar visible, para que el personal registre correctamente su acceso y salida del mismo.

3. El personal autorizado debe registrar su acceso y salida en la **Bitácora de Control de Accesos al Centro de Cómputo** de la Procuraduría Agraria.

4. Al final del día la **Bitácora de Control de Accesos al Centro de Cómputo** de la Procuraduría Agraria deberá ser cerrada con la firma de verificación del Jefe de Departamento de Telecomunicaciones, o el Subdirector de Soporte Técnico o el Director de Informática.

5. Las visitas que ingresen al Centro de Cómputo, invariablemente deberán ser acompañadas en todo momento por personal de la Dirección de Informática hasta el final de la visita.

6. Los proveedores externos de servicios y equipos de cómputo invariablemente deben registrar su acceso y salida en la **Bitácora de Control de Accesos al Centro de Cómputo** de la Procuraduría Agraria.

Del acceso al equipo de cómputo.

1. El Administrador de la Red es responsable del supervisar el adecuado uso, aprovechamiento y conservación de los equipos de cómputo y Servidores instalados en el Centro de Cómputo de la Procuraduría Agraria.

2. Las visitas deben abstenerse de operar cualquier equipo de cómputo o Servidor, con excepción del personal técnico de la Dirección de Informática, o bien, del personal técnico aprobado para las acciones de mantenimiento preventivo y, en su caso, del personal técnico designado por el fabricante o proveedor para realizar tareas de reparación, instalación y/o configuración.

3. El personal técnico autorizado y las visitas tienen totalmente prohibido fumar o ingerir todo tipo de bebidas mientras se encuentren el Centro de Cómputo de la Procuraduría Agraria.

4. El personal adscrito a la Dirección de Informática que disponga de la autorización para el acceso al Centro de Cómputo de la Procuraduría Agraria y a equipo de cómputo y Servidores de uso específico y misión crítica, invariablemente deben operarlos adecuadamente, para mantener óptimo estado físico y conservación.

5. Es responsabilidad de la Dirección de Informática la operación de todos los equipos y sistemas del Centro de Cómputo de la Procuraduria Agraria.

6. Los equipos de cómputo y Servidores estarán en función **las 24 horas los 365 días del año**, excepto las acciones de mantenimiento preventivo; los Servidores son los siguientes: Internet, Correo Electrónico, Base de Datos y Sistemas, Seguridad de Acceso, de Dominio, de FTP y de Respaldo Institucional.

De la creación y asignación de claves de acceso.

1. La elaboración y diseño de las claves de seguridad de acceso es actividad propia y única de la Dirección de Informática; en específico para los casos en que el usuario administrador del sistema institucional no cuente con la opción de crear el nombre de usuario y claves de seguridad.

2. Se diseñará una clave acceso de seguridad para el acceso a equipos de cómputo, para el acceso al correo electrónico institucional, para el acceso a las bases de datos de sistemas de información institucionales, para el acceso a los Servidores del Centro de Cómputo, para el acceso al servicio de telefonía y para aquellos servicios como carpetas compartidas en servidores, servidores FTP, Telefonía o equipos que por su naturaleza y función así lo exijan.

3. La Dirección de Informática se abstiene de cambiar, por motivos de seguridad, las claves de acceso a los Servidores, Servicios, Telefonía y el acceso a las Bases de Datos de los Sistemas de Información Institucionales.

4. La solicitud para el acceso a los servicios de Red, Correo Electrónico, las bases de datos de los sistemas de información institucionales y el servicio de telefonía, deberá realizarse a la Dirección de Informática mediante el formato de **Control de Claves de Acceso** firmado por el titular de la unidad administrativa correspondiente.

5. Las claves de acceso a servicios de Red, Correo Electrónico y las bases de datos de los sistemas de información institucionales se crearán mediante la asignación de un Usuario y una Clave de Seguridad de Acceso (**Password**), salvo aquellos casos que únicamente se requiera de Clave de Seguridad de Acceso (**Password**), como es el caso del las restricciones del Servicio de Telefonía.

6. La creación de las claves de seguridad se realizará de acuerdo a los modelos utilizados para cada Servicio o Sistema Informático, de acuerdo a las siguientes características:

    a. Longitud mínima de 4 campos.
    b. Longitud máxima, la soportada por la aplicación, sistema o servicio utilizado.
    c. Compuesta de “Caracteres Numéricos, Alfabéticos y Caracteres Especiales”
    d. Caracteres intercalados de manera aleatoria.

7. La asignación o entrega de las claves de acceso a lo servicios de Red como Internet, Correo Electrónico, Servidores de Dominio, FTP, Respaldo, Carpetas Compartidas y las Bases de Datos de los Sistemas de Información Institucionales se realizará mediante la entrega de ésta en sobre debidamente cerrado y dirigido al Director General de la Unidad solicitante.

8. La entrega del sobre cerrado se realizará en propia mano del titular de la unidad administrativa solicitante o de la persona que éste designe para el caso, firmando de conformidad de la entrega.

9. En aquellos casos que se requiera de la generación de una clave de acceso de seguridad temporal para acceso a los servicios y/o sistemas de información institucional, ésta será elaborada y proporcionada por la Dirección de Informática.

10. La solicitud de una clave de acceso de seguridad temporal deberá ser requerida mediante el formato de **Control de Claves de Acceso**, debidamente firmada por el titular de la unidad administrativa correspondiente y justificando su requerimiento.

11. La Dirección de Informática proporcionará mediante sobre cerrado y sellado la clave de seguridad de acceso al titular de la unidad administrativa, o bien, al usuario resguardante del bien informático.

12. El titular de la unidad administrativa o el usuario resguardante deberán firmar de conformidad la recepción del sobre cerrado y sellado que contiene la clave de acceso de seguridad temporal correspondiente.

De la actualización o cambio de claves de acceso.

1. La actualización o cambio de las claves de seguridad de acceso es actividad propia y única de la Dirección de Informática; en específico para los casos en que el usuario administrador del sistema institucional no cuente con la opción de crear el nombre de usuario y claves de seguridad.

2. La solicitud de actualización o cambio de claves de seguridad de acceso a los servicios de Red como Internet, Correo Electrónico, Servidores de Dominio, FTP, Respaldo, Carpetas Compartidas y las Bases de Datos de los Sistemas de Información Institucionales deberá solicitarse a la Dirección de Informática mediante el formato de **Control de Claves de Acceso** firmado por el titular de la unidad administrativa correspondiente.

3. La solicitud de actualización o cambio de claves de seguridad de acceso de servicios y/o sistemas de información institución, cuando los datos del usuario no correspondan al equipo de cómputo descrito en el formato de **Control de Claves de Acceso**.

4. La entrega de la clave de acceso a servicios y sistemas de información institucionales se proporcionará en sobre debidamente cerrado y sellado al titular de la unidad administrativa solicitante, o bien, al usuario resguardante del bien informático respectivo.

5. El titular de la unidad administrativa o el usuario resguardante deberán firmar de conformidad la recepción del sobre cerrado y sellado que contiene la clave de acceso de seguridad correspondiente.

6. La Dirección de Informática generará los cambios de claves de seguridad de acceso asignadas a los equipos de cómputo y de comunicaciones de uso específico y de misión crítica, por motivos de seguridad y resguardo de los servicios, programas de cómputo y bases de datos de los sistemas de información institucionales.

De la cancelación de claves de acceso.

1. La cancelación temporal o definitiva de las claves de seguridad de acceso es actividad propia y única de la Dirección de Informática; en específico para los casos en que el usuario administrador del sistema institucional no cuente con la opción de crear el nombre de usuario y claves de seguridad.

2. La solicitud de cancelación temporal o definitiva de claves de seguridad de acceso a los servicios de Red como Internet, Correo Electrónico, Servidores de Dominio, FTP, Respaldo, Carpetas Compartidas y las Bases de Datos de los Sistemas de Información Institucionales deberá solicitarse a la Dirección de Informática mediante el formato de **Control de Claves de Acceso**, firmado por el titular de la unidad administrativa correspondiente.

3. La solicitud de cancelación temporal o definitiva de claves de seguridad de acceso de servicios y/o sistemas de información institución, cuando los datos del usuario no correspondan al equipo de cómputo descrito en el formato de **Control de Claves de Acceso**.

4. La solicitud de cancelación temporal o definitiva de claves de seguridad de acceso a los servicios de Red como Internet, Correo Electrónico, Servidores de Dominio, FTP, Respaldo, Carpetas Compartidas y las Bases de Datos de los Sistemas de Información Institucionales deberá solicitarse a la Dirección de Informática mediante el formato de **Control de Claves de Acceso**, firmado por el titular de la unidad administrativa correspondiente.

5. Las unidades administrativas tienen la responsabilidad de requerir la baja temporal o definitiva de las claves de seguridad de acceso en los casos de separación del cargo o cambio de unidad de adscripción del usuario, por razones de seguridad e integridad de los servicios, sistemas de información y/o bienes informáticos.

6. La Dirección de Informática notificará mediante oficio debidamente firmado al titular de la unidad administrativa correspondiente sobre la cancelación temporal o definitiva de la clave de seguridad de acceso.

De la responsabilidad del usuario en el uso y resguardo de claves de acceso.

1. Los titulares de las unidades administrativas son los responsables de determinar los usuarios que tendrán acceso a los servicios, sistemas de información institucionales y equipos de cómputo; con la finalidad de requerir, mediante el formato de **Control de Claves de Acceso**, a la Dirección de Informática la clave de seguridad de acceso correspondiente.

2. La unidad administrativa responsable de cada sistema de información institucional establecerá las restricciones convenientes para su uso, consulta, actualización y generación de productos finales, con objeto de garantizar su integridad.

3. Es responsabilidad total y única del usuario el adecuado uso, aprovechamiento y resguardo de la clave de seguridad de acceso elaborada y proporcionada por la Dirección de Informática.

4. El usuario debe informar al titular de su unidad administrativa de adscripción el extravío de la clave de seguridad de acceso asignada para el uso de servicios, sistemas de información institucionales y/o equipos de cómputo; para evitar riesgos en la integridad de la infraestructura informática asignada.

5. Es responsabilidad del titular de cada unidad administrativa y del usuario de los servicios, sistemas de información institucionales y/o equipos de solicitar a la Dirección de Informática los movimientos de alta, actualización o baja de las claves de seguridad de acceso correspondientes.

6. Es responsabilidad de cada unidad administrativa y del usuario de los servicios. Sistemas de información institucionales de informar a la Dirección de Informática cualquier posible mal uso de la clave de seguridad de acceso asignadas.

Del resguardo del control de claves de acceso.

1. La Dirección de Informática invariablemente es responsable de integrar las claves de seguridad de acceso a los servicios, sistemas de información institucionales y equipos de cómputo (bienes informáticos y equipos de cómputo de uso específico y misión crítica asignada), con la finalidad de resguardarlas y asegurar la integridad de la infraestructura informática instalada.

2. El **Control Maestro de Claves de Acceso** es la herramienta donde se concentrarán las claves de seguridad de acceso a los servicios, sistemas de información institucionales y equipos de cómputo; el cual será resguardado en las instalaciones que ocupa el titular de la Dirección de Informática y una copia de dicho control en la Bóveda de Seguridad Bancaria.

3. El **Control Maestro de Claves de Acceso** se actualizará de acuerdo a los movimientos de alta, actualización o cancelación temporal o definitiva de claves de seguridad de acceso requeridas por las unidades administrativas de la Procuraduría Agraria.

4. Solamente tendrán acceso a la consulta del **Control Maestro de Claves de Acceso** el Director de Informática, el Subdirector de Soporte Técnico, el Jefe de Telecomunicaciones y en el caso de los Sistemas de Información Institucional el Subdirector de Procesamiento de Datos.

5. La información contenida en el **Control Maestro de Claves de Acceso** es considerada como confidencial, con la finalidad de resguardar la integridad de la infraestructura informática asignada e instalada en las unidades administrativas de la Procuraduría Agraria.

6. El **Control Maestro de Claves de Acceso** estará bajo resguardo y responsabilidad del Director de Informática, el cual está conformado de la siguiente manera:

   a. Carpeta de Consulta (impresión original de las claves de seguridad de acceso a servicios, sistemas de información y equipo de cómputo).

   b. Formato Electrónico (dispuesto con seguridad de acceso y oculto).

7. La actualización del **Control Maestro de Claves de Acceso** a los servicios, sistemas de información institucionales y equipos de cómputo queda a cargo de la Dirección de Informática mediante la Subdirección de Soporte Técnico para el caso de los servicios y equipo de cómputo; y de la Subdirección de Procesamiento de Datos para las bases de datos de los sistemas de información institucionales.

8. La actualización del resguardo del **Control Maestro de Claves de Acceso** a los servicios, sistemas de información institucionales y equipo de cómputo en la Bóveda de Seguridad Bancaria queda bajo la responsabilidad de la Dirección de Informática, quien designará a los funcionarios que serán debidamente registrados ante la Institución Bancaria para el traslado del Control Maestro a la Bóveda de Seguridad Bancaria.

EQUIPO DE SEGURIDAD.

Implementar un área específica para la instalación del Centro de Cómputo, el cual disponga de las medidas de seguridad para la detección y extinción de incendios, clima adecuado y instalaciones eléctricas y medidas del tráfico de personal; para asegurar la integridad física de la infraestructura instalada.

Del equipo de detección y extinción de incendios.

1. La Dirección de Informática debe definir las características y especificaciones técnicas adecuadas para requerir a la Dirección de Recursos Materiales y Servicios la adquisición de un equipo de detección y extinción de incendios.

2. La Dirección de Informática debe supervisar la correcta instalación del equipo de detección y extinción de incendios, así como, de verificar su óptimo funcionamiento.

3. La Dirección de Informática debe requerir la contratación del mantenimiento preventivo y correctivo del equipo de detección y extinción de incendios, así como, establecer el calendario de eventos que debe realizar el proveedor externo de mantenimiento y verificar, una vez concluidas las acciones de mantenimiento, su óptimo funcionamiento.

4. La Dirección de Informática debe coordinar las acciones de las revisiones, capacitación y uso del equipo de detección y extinción de incendios con el Personal de Vigilancia en turno.

5. Es responsabilidad del Jefe de Telecomunicaciones supervisar la correcta operación del equipo de detección y extinción de incendios ubicados en el Centro de Cómputo y Conmutador Central, con la finalidad de asegurar su óptimo funcionamiento.

6. El Jefe de Telecomunicaciones debe registra en la **Bitácora de Revisión de Equipos de Seguridad** los eventos que se realicen de mantenimiento (efectuado por personal externo) y revisión (realizado por él mismo); en las fechas programadas.

Del aire acondicionado.

1. La Dirección de Informática debe definir las características y especificaciones técnicas adecuadas para requerir a la Dirección de Recursos Materiales y Servicios la adquisición de un equipo de clima artificial.

2. La Dirección de Informática debe supervisar la correcta instalación del equipo de clima artificial, así como, de verificar su óptimo funcionamiento.

3. La Dirección de Informática debe requerir la contratación del mantenimiento preventivo y correctivo del equipo de clima artificial, así como, establecer el calendario de eventos que debe realizar el proveedor externo de mantenimiento y verificar, una vez concluidas las acciones de mantenimiento, su óptimo funcionamiento.

4. Es responsabilidad del Jefe de Telecomunicaciones supervisar la correcta operación del equipo de clima artificial ubicado en el Centro de Cómputo y Conmutador Central, con la finalidad de asegurar su óptimo funcionamiento.

5. El Jefe de Telecomunicaciones debe registra en la Bitácora de **Revisión de Equipos de Seguridad** los eventos que se realicen de mantenimiento (efectuado por personal externo) y revisión (realizado por él mismo); en las fechas programadas.

De la unidad de respaldo de energía (UPS).

1. La Dirección de Informática debe definir las características y especificaciones técnicas adecuadas para requerir a la Dirección de Recursos Materiales y Servicios la adquisición de una unidad de respaldo de energía (UPS).

2. La Dirección de Informática debe supervisar la correcta instalación de la unidad de respaldo de energía (UPS), así como, de verificar su óptimo funcionamiento.

3. La Dirección de Informática debe requerir la contratación del mantenimiento preventivo y correctivo de la unidad de respaldo de energía (UPS)., así como, establecer el calendario de eventos que debe realizar el proveedor externo de mantenimiento y verificar, una vez concluidas las acciones de mantenimiento, su óptimo funcionamiento.

4. Es responsabilidad del Jefe de Telecomunicaciones supervisar la correcta operación de la unidad de respaldo de energía (UPS). ubicado en el Centro de Cómputo y Conmutador Central, con la finalidad de asegurar su óptimo funcionamiento.

5. El Jefe de Telecomunicaciones debe registra en la Bitácora de **Revisión de Equipos de Seguridad** los eventos que se realicen de mantenimiento (efectuado por personal externo) y revisión (realizado por él mismo); en las fechas programadas.

De la planta de energía.

1. La Dirección de Informática debe definir las características y especificaciones técnicas adecuadas para requerir a la Dirección de Recursos Materiales y Servicios la adquisición de una planta de energía.

2. La Dirección de Informática debe supervisar la correcta instalación de la planta de energía, así como, de verificar su óptimo funcionamiento.

3. La Dirección de Informática debe requerir la contratación del mantenimiento preventivo y correctivo de la planta de energía, así como, establecer el calendario de eventos que debe realizar el proveedor externo de mantenimiento y verificar, una vez concluidas las acciones de mantenimiento, su óptimo funcionamiento.

4. El Jefe de Telecomunicaciones debe registra en la Bitácora de **Revisión de Equipos de Seguridad** los eventos que se realicen de mantenimiento (efectuado por personal externo) y revisión (realizado por él mismo); en las fechas programadas.

SUPERVISIÓN Y MONITOREO.

Realizar un monitoreo constante de los equipos de cómputo y servicios de uso específico y designados con una misión crítica, con la finalidad de disponer de una herramienta que asegure su correcto funcionamiento.

De los equipos y servicios críticos.

1. La Dirección de Informática establecerá las siguientes acciones necesarias para realizar los monitoreos de los equipos de cómputo y servicios de uso específico y designados con una misión crítica, para asegurar su operación y rendimiento.

2. Las revisiones que se realicen a los equipos de cómputo y servicios de uso específico y designados con una misión crítica deben estar orientadas a aspectos de seguridad lógica y física, de acuerdo al horario establecido para tales efectos.

3. El Jefe de Telecomunicaciones tiene la responsabilidad de realizar un monitoreo (al inicio de las actividades 9:00 horas, en el punto de mayor actividad 14:00 horas y a las 18:00 horas) de los equipos de cómputo y servicios de uso específico y designados con una misión crítica, a efecto de asegurar su óptimo funcionamiento.

4. El Jefe de Telecomunicaciones debe registrar en la Bitácora de **Monitoreo de Equipos de Cómputo y Servicios Críticos**, el resultado del monitoreo que realice.

5. El Jefe de Telecomunicaciones debe registrar en la Bitácora de **Fallas en los servicios de la Red Institucional**, así como reportar al Centro de Atención del Servicio correspondiente para implementar las medidas necesarias para recuperar su óptimo funcionamiento.

6. La Dirección de Informática debe elaborar un Plan de Contingencias que esté acorde a las actividades críticas, a efecto de asegurar la operación de los equipos de cómputo y servicios de uso específico y designados con una misión crítica.

SERVIDORES DE APOYO EN RED.

Implementar servicios de apoyo en red como los de Servidores FTP, WEB, Respaldo y Archivos Compartidos, esta orientado brindar un mejor uso y aprovechamiento de las facilidades y herramientas con que cuenta la Procuraduria Agraria.

De la asignación de espacio y servicios en Servidores.

1. La Dirección de Informática es la responsable de la asignación de espacios y servicios de la Red de la Procuraduria Agraria, de acuerdo a disponibilidad y seguridad de los equipos, servicios y sistemas de información Institucional.

2. Los requerimientos de espacios o servicios deberán realizarse de acuerdo al formato de **Requerimientos de Espacios y Servidores en Servidores de Red**, dirigido al Director de Informática y firmado por el Titular del área solicitante.

3. La Dirección de Informática se reserva el derecho de la asignación de espacios o servicios de acuerdo a la disponibilidad de los mismos.

4. Una vez asignado el espacio o servicio al área solicitante, ésta será responsable directa sobre el uso del espacio o servicio solicitado.

5. Será responsabilidad del área solicitante el tipo de información que ingrese en los espacios solicitados.

6. Será responsabilidad del área solicitante la actualización o en su caso la baja de la información contenida en los espacios asignados por la Dirección de Informática a través del formato **Requerimientos de Espacios y Servidores en Servidores de Red**.

7. Será responsabilidad del área solicitante el correcto uso de las claves de seguridad asignada para el acceso a espacios o servicios.

SANCIONES.

1. Cualquier violación a la Normatividad y Lineamientos para el uso de las Claves de Seguridad de Acceso a servicios, sistemas de información institucionales y equipos de cómputo deberá ser sancionada con base al nivel de daño y riesgo para la integridad de la infraestructura informática Institucional.

2. Las sanciones pueden ser desde un escrito con copia al expediente del usuario, el retiro del bien informático o la suspensión del servicio correspondiente, hasta una sanción económica, dependiendo de la gravedad de la falta cometida.

3. Todas las acciones que no estén previstas y que en su momento comprometan la seguridad e integridad de la infraestructura informática Institucional será revisada por la Dirección de Informática, quien emitirá un dictamen técnico el cual será sometido al Comité de Informática y éste emitirá una resolución definitiva.

El usuario que no cumpla con la normatividad y lineamientos para el uso de las Claves de Seguridad de Acceso a servicios, sistemas de información institucionales y equipos de cómputo, será acreedor a las siguientes sanciones:

a. En la primera incidencia, se elaborará un escrito dirigido al usuario infractor con copia a su expediente y otra para el titular de la unidad administrativa de adscripción, indicando las fallas y omisiones que originan problemas en el bien y/o servicio de cómputo.

b. En la segunda incidencia, se realizará de manera inmediata el retiro del bien y/o servicio de cómputo, notificando, por escrito al titular de la unidad administrativa con copia para el Órgano Interno de Control y el usuario infractor, los motivos por los cuales se efectúa el levantamiento del equipo de cómputo.

c. Las sanciones económicas serán definidas por el Comité de Informática de la Procuraduría Agraria, con base al dictamen técnico emitido por la Dirección de Informática.

Las sanciones son de aplicación general, toda vez que implican daños a la infraestructura informática propiedad de la Procuraduría Agraria, tanto a los equipos de cómputo, como a los servicios de comunicación.